Bescherming persoonsgegevens

84

Naar een betere bescherming van de gegevens van het Rijksregister van natuurlijke personen

Recent zijn de modaliteiten voor het gebruik van het identificatienummer van het Rijksregister van natuurlijke personen aangepast. Het Rijksregister is, zoals de gemeentelijke basisadministratie persoonsgegevens in Nederland, de authentieke bron met de identificatiegegevens van de natuurlijke personen die op het Belgische grondgebied verblijven, met dien verstande dat het centraal wordt beheerd. De toegang tot de informatiegegevens in dat register wordt strikt wettelijk geregeld, waarbij de categorieën van mogelijke gerechtigden worden opgesomd in de wet. Controle hierop wordt voorafgaandelijk verricht door het Sectoraal Comité van het Rijksregister. Dit is een comité dat is opgericht in de schoot van de Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL), de Belgische tegenhanger van het College bescherming persoonsgegevens. De toegang tot de informatiegegevens in het Rijksregister wordt daarbij onderscheiden van het gebruik van het identificatienummer van het Rijksregister, het Belgische equivalent van het burgerservicenummer. Dit houdt in dat wie toegang heeft tot de gegevens, niet automatisch het nummer mag gebruiken en omgekeerd. Dit onderscheid is ingegeven door het risico dat verbonden is aan het gebruik van het nummer, met name om koppelingen te maken. Maar in de praktijk blijkt dat dit onderscheid soms ook kan leiden tot een mindere bescherming.

Wie toegang heeft en het nummer mag gebruiken, kan de gegevens van een persoon opzoeken op basis van diens identificatienummer. Dat maakt het mogelijk dat enkel de gegevens van de betrokken persoon worden geraadpleegd. Voor wie toegang heeft, maar niet het recht om het identificatienummer te gebruiken, verloopt de bevraging noodzakelijkerwijze anders. Zij kunnen het Rijksregister enkel raadplegen door middel van 'gerichte' opzoekingen. Zo'n zoekopdracht gebeurt hetzij via de naam (de 'fonetische' opzoeking), hetzij via het adres, hetzij via de geboortedatum. Risico hierbij is dat men hierdoor gegevens raadpleegt van verschillende andere personen, waar men niet toe gerechtigd is.

Zowel de CBPL als het Sectoraal Comité zijn daarom al enige tijd vragende partij om deze situatie bij te sturen. De bevoegde minister heeft nu de gewenste bijsturing doorgevoerd. Ze bestaat erin dat wie gemachtigd is om toegang te hebben zonder het Rijksregisternummer te mogen gebruiken, thans de toelating krijgt om dat identificatienummer toch intern in zijn bestanden op te nemen. Op die manier verschijnen bij een latere raadpleging enkel de gegevens van de betrokken persoon. Die bijsturing neemt de vorm aan van een koninklijk besluit, waarbij de gevallen worden vastgelegd waarin een machtiging tot gebruik van het identificatienummer niet vereist is. Deze mogelijkheid en de basis daartoe vindt men in de Wet op het Rijksregister zelf. Daarbij worden wel een aantal voorwaarden opgelegd. Vooreerst mag enkel het identificatienummer van de persoon op wie de zoekopdracht betrekking heeft, worden opgenomen. Vervolgens mag dit nummer enkel worden opgenomen met het oog op gebruik bij een latere zoekopdracht. Gebruik van het nummer voor enig ander doel blijft onderworpen aan de normale procedure en vereist een machtiging door het Sectoraal Comité.

Op deze manier wordt een ongewild gevolg van een privacybeschermende maatregel rechtgezet en aldus de bescherming van de burger meer kracht bijgezet. (DDB)

Bron: KB van 24 november 2010 tot vastlegging van de gevallen waarin een machtiging tot gebruik van het identificatienummer van het Rijksregister niet vereist is, Belgisch Staatsblad 18 januari 2011 (2e editie); advies RR nr. 01/2009 van 22 april 2009 van het Sectoraal Comité van het Rijksregister met betrekking tot het ontwerp van koninklijk besluit tot vastlegging van de gevallen waarin een machtiging tot gebruik van het identificatienummer van het Rijksregister niet vereist is, raadpleegbaar via de website <www.privacycommission.be> onder de rubriek adviezen bij het trefwoord Sectoraal Comité van het Rijksregister; 'Gegevens Rijksregister beter beschermd', De Juristenkrant 9 februari 2011, nr. 223

85

Privacycommissie doet aanbeveling over mobile mapping

De Belgische Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL) publiceerde eind 2010 een aanbeveling uit eigen beweging over mobile mapping. Het gaat hier om een algemene aanbeveling die geen effect heeft voor specifieke dossiers zoals Google Street View. De CBPL ziet mobile mapping als een technologie waarbij een voertuig uitgerust wordt met een camera en/of een scanner en hierbij data betreffende een specifieke weg digitaal kan opnemen, bijvoorbeeld door middel van 360°-foto's. Het gebruik van dergelijke technologie kan verschillende doeleinden dienen. De meest voor de hand liggende voorbeelden – volgend uit onder meer Google Street View – zijn het gebruik voor navigatie en toerisme. Ook de overheid kan dergelijke technologie aanwenden om op elk moment de werkelijke terreinsituatie te bekijken. Zo kan de overheid beter en sneller situaties inschatten zonder hiertoe steeds een terreinbezoek te moeten voorzien. Ook voor de schatting van onroerend goed kan mobile mapping een goede eerste indruk geven.

Net omdat voertuigen uitgerust voor mobile mapping alle informatie rondom zich waarnemen en opslaan, is er het risico dat hierbij ook informatie betreffende personen, hun voertuigen en hun woningen ingezameld wordt. Gelet op de kwaliteit van de ingezamelde beelden en de mogelijke gevoelige aard van de informatie – bijvoorbeeld een

persoon die gefilmd wordt aan een bepaalde dokterspraktijk – ziet de CBPL dit als mogelijke persoonsgegevens. De CBPL ziet mobile mapping daarom als een potentiële verwerking van persoonsgegevens, die daarom onderworpen is aan de beginselen van de Belgische Privacywet.

De verwerking van gegevens verzameld via mobile mapping moet daarom rechtmatig en proportioneel verlopen. Gegevens mogen slechts voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verwerkt. De CBPL wijst hier ook nadrukkelijk op de transparantieplicht. Betrokkenen moeten voldoende ingelicht worden over de wijze van de verwerking, de doeleinden van de verwerking en de aard van de persoonsgegevens die verwerkt worden. Een aangifte bij de CBPL is nodig om te beoordelen of de verwerking op voldoende wijze geproportioneerd wordt. Wat de rechtmatigheid van de verwerking betreft wijst de CBPL op de praktische onmogelijkheid om de toestemming van elke betrokkene te verkrijgen. Er zal daarom vooral beroep gedaan worden op de mogelijkheid van het gerechtvaardigd belang dat zwaarder doorweegt dan de belangen of de fundamentele rechten en vrijheden van de betrokkene. Hierbij merkt de CBPL op dat het specifieke doel van de verwerking voor ogen gehouden moet worden. Indien personen, hun voertuigen en hun woningen onherkenbaar gemaakt worden, bijvoorbeeld door blurring, zal het belang van de betrokkene minder zwaar doorwegen dan het belang van de aanbieder van de diensten van mobile mapping. Indien het echter de bedoeling is dat personen op herkenbare wijze geregistreerd worden en dat deze data aldus publiek toegankelijk gemaakt wordt, bijvoorbeeld via het internet, dan zal uiteraard het belang van de betrokkene zwaarder doorwegen.

Wat betreft de informatieplicht van de verantwoordelijke voor de verwerking, stelt de CBPL een algemene en verstaanbare informatienota voor, waaruit de betrokkenen zowel online als offline voldoende informatie kunnen putten. Verder raadt de CBPL nog aan om een 'privacy assessment' uit te voeren, om aldus de precieze implicaties van mobile mapping op de privacy en bescherming van persoonsgegevens in te kunnen schatten. Ook de toepassing van 'security and privacy by design' wordt ten zeerste aangeraden. (NV)

Bron: Commissie voor de bescherming van de persoonlijke levenssfeer, 'Aanbeveling uit eigen beweging 05/2010 inzake Mobile Mapping (CO-AR-2010-007)', 15 december 2010, <www.privacycommission.be>, 9 p.

86

Opinie Privacycommissie over beheer centrale registers testamenten en huwelijksovereenkomsten

De Belgische Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL) sprak zich recent uit over het voorontwerp van een koninklijk besluit betreffende het beheer van de centrale registers van testamenten en huwelijksovereenkomsten. Het doel van dit koninklijk besluit is het bepalen van de precieze gegevens betreffende de huwelijksovereenkomsten en testamenten die opgenomen kunnen worden in een centraal register, alsook het regelen van de toegang tot dergelijk centraal register. Waar voor testamenten al sinds 1977 een dergelijk register bestaat, bestaat het juridisch kader voor een centraal register voor huwelijksovereenkomsten slechts sinds 2009. De CBPL merkt hierbij op dat er wel al een aantal bepalingen bestaan die tot op zekere hoogte de openbaarheid van het huwelijksstelsel regelen.

Een eerste belangrijke opmerking van de CBPL is dat de programmawet die het centraal register voor huwelijksovereenkomsten voorziet geen melding maakt van de doeleinden waarvoor dergelijk register opgericht zou moeten worden. Voor testamenten kan het doel gevonden worden in het Verdrag van Bazel van 1972, maar voor huwelijksovereenkomsten kan men enkel vaststellen dat het doeleinde van dergelijk register afwijkt van het doel van het centraal register voor testamenten. De CBPL raadt daarom aan om dergelijke doeleinden minstens in het Verslag aan de Koning te verduidelijken.

Hoewel het voorontwerp van KB wel aangeeft dat de Koninklijke Federatie van het Belgisch Notariaat belast wordt met het beheer van het centraal register, wordt hier niet expliciet aangehaald dat deze federatie de verantwoordelijke voor de verwerking is. Krachtens de Privacywet moet de verantwoordelijke immers expliciet aangeduid worden. Daarnaast raadt de CBPL ook aan om de lijst met gegevens die in het register zullen worden opgenomen, te verduidelijken. Dergelijke verduidelijking kan niet in het huidige voorontwerp van KB gevonden worden. Wel voorzien is een lijst met minimale gegevens die door de notaris meegedeeld moet worden voor de inschrijving in het register.

Opvallend is dat het voorontwerp voorziet in een afwijking op de machtigingsbevoegdheid van de Sectorale Comités van het Rijksregister en van de Sociale Zekerheid en van de Gezondheid. Dergelijke afwijking is mogelijk, zij het slechts op expliciete wijze, mits goede motivering en na een in de ministerraad overlegd koninklijk besluit. De vereiste motivatie is hier echter niet aanwezig.

Wat de toegang tot het register van testamenten betreft, wordt bepaald dat de notaris de betrokken erfgenamen moet opsporen. Voor het register van huwelijksovereenkomsten wordt bepaald dat de openbare overheden, instellingen van openbaar nut en instelling van algemeen belang in het kader van de uitvoering van hun wettelijke opdracht – na positief advies van de CBPL – toegang krijgen tot dit register. De CBPL vraagt hierbij te verduidelijken dat de toegang van de overheid slechts toegelaten kan zijn wanneer de kennisneming van het huwelijksstelsel van een persoon strikt noodzakelijk is voor de uitvoering van de opdracht van openbare dienst van de overheid. De CBPL vraagt bovendien om de precieze omstandigheden waarin toegang

gevraagd kan worden, te verduidelijken of om de bevoegde minister een besluit te laten uitvaardigen dat dergelijke omstandigheden vermeldt. De noodzakelijkheid van de aanvraag moet volgens de CBPL steeds gemotiveerd worden. Daarnaast zou een specifiek recht op toegang voor de betrokkenen verleend kunnen worden teneinde de transparantie van dergelijk register te verhogen.

De CBPL is geen voorstander om de aanvrager van informatie uit het register te machtigen tot het gebruik van het Rijksregisternummer als zoeksleutel. De algemene formulering van de bepaling in haar huidige vorm doet afbreuk aan de machtigingsbevoegdheid van het Sectoraal Comité van het Rijksregister. Een gelijkaardige redenering wordt gevolgd voor een bepaling die de Koninklijke Federatie van het Belgisch Notariaat machtigt tot toegang tot het Rijksregister. Ook een specifieke bepaling die de betrokkenen het recht op verbetering biedt is volgens de CBPL overbodig in het licht van de reeds bestaande bepalingen in de Privacywet. Hetzelfde geldt voor een bepaling betreffende de beveiliging van de in de registers verwerkte persoonsgegevens. Wat de beveiliging betreft wordt wel nog een nauwkeurig loggingsysteem aangeraden, om te bewaren wie op welk moment welke gegevens heeft geraadpleegd.

Gelet op de hier aangehaalde kritische punten gaf de CBPL een ongunstig advies mee voor dit voorontwerp van koninklijk besluit. Een gunstig advies is slechts mogelijk na een verdere redactie van de tekst met implementatie van de door de CBPL aangehaalde opmerkingen. (NV)

Bron: Commissie voor de bescherming van de persoonlijke levenssfeer, 'Advies 29/2010 bij het voorontwerp van koninklijk besluit betreffende het beheer van de centrale registers van testamenten en huwelijksovereenkomsten (CO-A-2010-027)', 15 december 2010, <www.privacycommission.be>, 8 p.

Internationaal

87

Opinie Europese Toezichthouder voor Gegevensbescherming over Europees onderzoeksproject Turbine

Op 1 februari 2011 publiceerde de Europese Toezichthouder voor gegevensbescherming voor het eerst een opinie over een onderzoeksproject dat door de Commissie werd gefinancierd. De Toezichthouder deed dit in het kader van haar beleidspaper van 2008 over de rol van de Toezichthouder en Europees onderzoek en technologische ontwikkelingen. De bedoeling van de Toezichthouder is om het 'privacy by design'-principe binnen Europese onderzoeksprojecten te promoten en te ondersteunen. Zijn opinie heeft daarbij niet alleen betrekking op de technische ontwikkelingen van het project, maar ook op de onderzoeksmethodologie en procedures die in het project ontwikkeld worden.

Het Europees project Turbine (2008-2011) had tot doel om op het gebied van privacyvriendelijk gebruik van vingerafdrukken innovatieve technologie te ontwikkelingen en dit te demonstreren. Zoals ondertussen langzamerhand bekend, is biometrie gebaseerd op unieke kenmerken van personen. De verwerking van biometrische gegevens kent specifieke risico's, onder meer omdat deze kenmerken gevoelige informatie kunnen bevatten, personen identificeren, toelaten om andere informatie over de betrokken persoon met elkaar te koppelen en niet kunnen vervangen worden in geval van misbruik. De Toezichthouder herinnerde aan eerdere opinies waarin hij benadrukte dat omwille van de specifieke aard van biometrische gegevens, deze speciale risico's moeten getemperd worden en dat het gebuik en de verwerking van biometrische gegevens moet gepaard gaan met consistente en sterke waarborgen. Het protocol en de technologie ontwikkeld binnen Turbine heeft betrekking op de transformatie van vingerafdrukken waarbij verschillende biometrische pseudo-identiteiten worden gecreëerd, die niet kunnen teruggerekend worden naar de oorspronkelijke vingerafdruk en die niet met elkaar kunnen verbonden worden. Het is ook mogelijk om de pseudo-identiteiten te herroepen en dus nieuwe uit te vaardigen. De Toezichthouder beschouwde deze twee eigenschappen van de ontwikkelde technologie, met name de niet-terugrekenbaarheid en de herroepbaarheid van de biometrische pseudo-identiteiten, belangrijk voor de verwerking van biometrische gegevens in overeenkomst met de gegevensbeschermingswetgeving om de redenen in de opinie verder toegelicht.

De Toezichthouder merkte ook op dat de wettelijke aspecten inzake het gebruik van biometrische gegevens door de projectpartners zeer ernstig werden genomen. Dit bleek ondermeer uit het feit dat de juridische aspecten en vereisten van bij de aanvang van het project, samen met de functionele en technische eisen, werden geanalyseerd, bestudeerd, gedocumenteerd en besproken.

De best practices die in het project ontwikkeld werden, werden eveneens onderzocht. De Toezichthouder is van mening dat de best practices nuttig zijn voor elk identiteitsmanagementsysteem dat zich aan de gegevensbeschermingswetgeving dient te houden. Het bepalen van het niveau van de accuraatheid van een biometrisch systeem dient weliswaar hierbij ook bepaald en opgevolgd te worden. De voorgestelde best practices laten ook toe om meer privacyvriendelijke systemen te ontwikkelen indien ze van bij het begin van het project in acht worden genomen. Het gebruik van eigen en publieke biometrische onderzoeksdatabanken werd eveneens onderzocht. De Toezichthouder adviseerde dienaangaande om ook de herkomst van publieke biometrische onderzoeksdatabanken te onderzoeken.

De Toezichthouder was positief over het project, de ontwikkelde technologie, de wijze waarop het onderzoek gevoerd en geïmplementeerd werd en het daarin gedemon-